H. Roßnagel, C.H. Schunck, J. Günther (Hrsg.): Open Identity Summit 2023,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 147

Exploring the Human Factor in IT-security: A mobile lab for Investigating User Behavior

Nicolas Fähnrich[1] Kevin Köster[2] Patrick Renkel[3] Richard Huber[4] Nadja Menz[5]

Abstract: The threat of cybersecurity incidents is increasingly challenging for companies and employee interaction plays a crucial role in the majority of cyberattacks. In this paper, we present a mobile, scalable IT-security lab to investigate the human factor in such incidents. The lab enables study participants to experience cyberattacks in an immersive workplace environment. In order to ensure that the target group of small and medium sized company (SME) employees is reached, we have designed the mobile lab in such a way that it can be easily operated in different locations and sizes.

Keywords: IT-security; cybersecurity; cyberattacks; mobile lab; human factor; SME

1 Introduction

Over the past few years, the financial damages caused by IT-security incidents for companies have increased and amounted to 203 billion € in 2022 in Germany [Be22; Hi17]. About 84% of all companies in Germany are affected and the respective cyberattacks are becoming increasingly professional[Hi17]. A closer look at the attack vectors used in successfully carried out cyberattacks reveals that the majority require user interaction, thus the human factor playing a decisive role in IT-security. Although the topic of IT-security is present in the media and a wide range of IT-security guidelines [Bu21; IS22], and security offers exist to increase the company's IT-security level, the threat of cyberattacks is becoming increasingly tense. We assume that companies and especially small and medium sized companies (SMEs) focus mainly on technical measures or that the chosen organizational measures like employee trainings and directives don't provide sufficient effectiveness to avoid IT-security incidents. In this paper we present a method to investigate the human factor in cyberattacks by using a mobile, scalable IT-security lab that enables study participants to experience realistic cyberattacks on a typical workstation in an immersive workplace environment. With our lab we are able to measure how likely it is for an SME to fall victim to a cyberattack, based on the preparedness and knowledge of SME employees which in turn is an indicator of the company's IT-security awareness and the current level of IT-security.

[1] Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart, nicolas.faehnrich@iao.fraunhofer.de
[2] Universität Hamburg, Department of Informatics, Vogt-Kölln-Straße 30, 22527 Hamburg, kevin.koester@uni-hamburg.de
[3] Hochschule Darmstadt, Department of Informatics, Schöfferstraße 3, 64295 Darmstadt, patrick.renkel@h-da.de
[4] Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, richard.huber@fokus.fraunhofer.de
[5] Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, nadja.menz@fokus.fraunhofer.de

doi:10.18420/OID2023_14

2 Related work

In a recent study the Department for Culture, Media and Sport in the United Kingdom [Fi18] showed that 74% of businesses see cybersecurity as a high priority, but 43% reported a breach in the last 12 months. About half of the businesses affected attributed it to fraudulent emails or websites. However, only 18% invested in additional training and only 9% adjusted their policies, while 28% did nothing at all. This shows that the threat an uneducated user represents is still extremely underestimated by management.

Studies by Sheng et al. [Sh10] and McCormac et al. [Mc17] both concluded, that the older and the more risk averse a person is, the less likely they fall for phishing attempts. Although in these studies anti-phishing education reduced the amount user become a victim by 40%, many security awareness campaigns still fail. Bada et al. [BSN19] analyzed why these campaigns fail. The main points are badly designed policies and systems in companies, as well that people might know the correct answers to security related questions, but don't act on them. Most awareness approaches can't directly influence the first point. Conventional campaigns might fail due to the second problem. Just knowing the problem, doesn't mean the employees act on them.

There are many approaches to teach users about security which are based on different kind of games [Gj17; PJA21; Sc18]. But in those games, players might get exposed for not knowing certain security measures and thus might be reluctant to play those games. A different approach was developed by Ghafir et al. [Gh18] in form of a security awareness framework which can display security related information based on the current application. This includes logging into a website or executing a file, so that the users is informed what consequences their action could have.

In our approach however, users are expected and encouraged to make mistakes. There is no penalty for doing anything wrong. This way users can actually experience how those attacks look like and what they actually do on a real system.

To the best of our knowledge, we are the first to create such a realistic scenario.

3 A mobile lab for investigating human driven cyberattacks

Conventional study approaches are usually based on a stationary laboratory environment that depicts a working environment only to a limited extent. In addition, there is the problem of finding enough study participants that correspond to the target group. E.g. university students often participated in similar studies. Educational online courses on the subject of IT-security often reach the target group however only partially depict a realistic working environment. For this reason, the requirements of the lab were in particular the realization of a realistic working environment including a workstation with business applications and processes typically found in SMEs. Furthermore, to be able to conduct representative studies

the test persons must correspond to the profile of the target group - employees of SMEs from different company divisions and positions - to the greatest possible extent. To achieve this, the lab had to be mobile and scalable in size depending on the site of installation. Possible locations are, for example, company, fair and event locations. The mobile lab is designed to investigate the processes of various attack vectors involving human interaction on the attacked company's site. Furthermore, a learning platform is provided and enables us to measure the effectiveness and efficiency of knowledge transfer.

The mobile lab is part of the project ELITE[EL22] and funded by the Federal Ministry for Economic Affairs and Climate Action (BMWK). It is built based on a truss system to be able to mount the hardware components and workstations while ensuring efficient assembly and transportation. A software platform was developed as a link between the experience of demonstrators and supporting learning content. It enables users to consolidate and internalize the experience of the demonstrators with the help of the learning materials. The platform is designed in such a way that it can be operated independently by users as well as guided by a supporting person. It is also publicly accessible so that users can access all learning materials even after completing demonstrators and regardless of their location. However, the demonstrators are only accessible if the so-called Nativeapp has been installed on the system used beforehand. The platform consists of a modern website connected to a Learning Management System (LMS). With the help of JavaScript, the platform can address the Nativeapp installed on the host and manage the demonstrations. Communication between the two elements takes place using https. The Nativeapp is a Python program and is installed on the system with all the necessary components using an installation script to ensure easy installation. This includes Docker containers of each demonstrator and all other components that each demonstrator needs to be functional. When a demo is started through the platform, the platform sends a command to the previously installed Nativeapp to start the appropriate Docker containers and prepare the system for the demonstrator. This can involve creating files, using user profiles for specific programs, entering host entries, and more. For this, the Nativeapp interacts, for security reasons, with the admin component, this component only takes care of actions that may only be performed by an admin. This structure has the effect that the development costs and the general maintenance effort can be kept low, because the software for the frontend can be chosen arbitrarily, as long as it is possible to integrate customized JavaScript. In addition, all software components are open source and can therefore be operated independently by companies. Thus, the platform and demonstrators can be adapted to the needs of individual companies and further demonstrators can be added or demonstrators that are not required can be removed.

The developed demonstrators cover several attack vectors relevant for companies and especially SMEs. This includes among others the following techniques in different scenarios: spear phishing attacks, malicious e-mail attachments, drive-by downloads, ransomware attacks, USB keystroke injection, man in the middle attacks and WIFI attacks.

In the following, the process of a ransomware demonstrator is described in detail: The user starts the demonstrator using the software platform installed on the machine. After a brief

introduction about the demonstrator and the role as an employee of a fictional company the system is prepared: an email-client is started, several documents are generated in the user directory including the desktop. An e-mail server is started and sends a spoofed e-mail to the user's mail account with a malicious file. The attacker impersonates a coworker of the fictional company and asks to check the attached document. When the user opens the document an error message is shown telling the user to activate the macros of the file. After the macros are activated, malicious code is executed that downloads and executes a ransomware that encrypts the previously generated files and displays a ransom note.

4 First insights from a test setup

As part of a first test setup of the mobile lab on the Hannover fair 2022 we conducted structured interviews with test persons after completing a demonstrator. We have asked for the individual assessment using a 1-5 Likert scale. As shown in Figure 1 most of the participants have rated their knowledge in IT and IT-Security with 3.43 and 2.79 as high and medium.

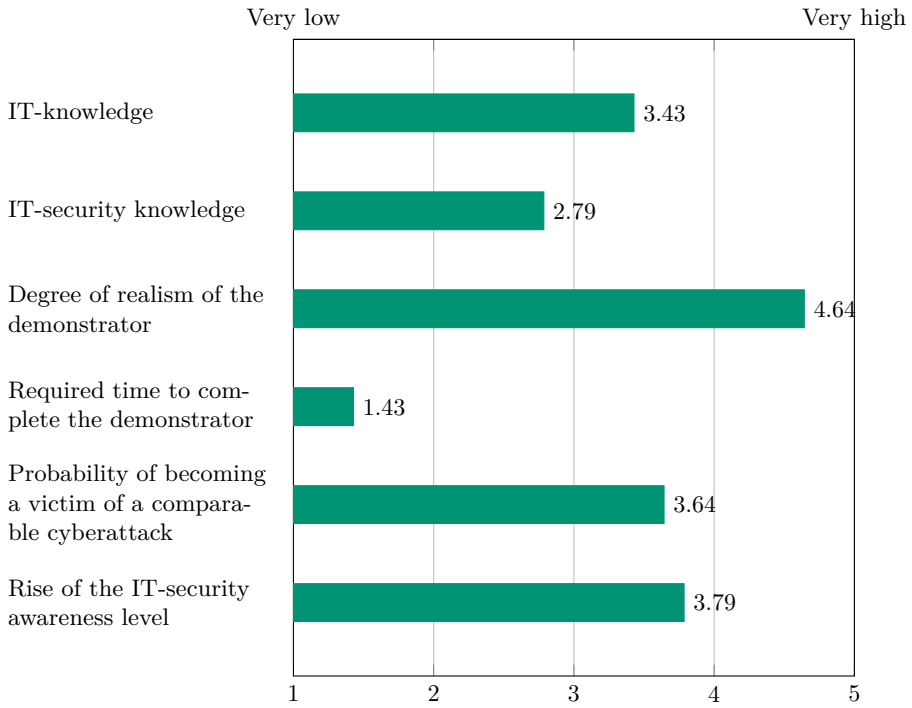

Fig. 1: Interview results (n=14)

The degree of realism of the used demonstrators was rated with 4.64 as very high. The required time to complete the demonstrator was rated with 1.43 and shows that the design

of the demonstrators does not exceed the attention span of the target group. The probability of becoming a victim of a comparable real cyberattack was rated with 3.65, indicating that there is a need for appropriate employee trainings in IT-security and especially cyberattacks that involve social engineering techniques. The rise of the personal awareness regarding IT-security and cyberattacks was rated with 3.79 as high. The results show that the the participants likely would have been victims of a cyber attack in a comparable real scenario even though the IT-knowledge is rated relatively high and the expertise in IT-security is rated medium. This shows that the participants are less well protected from common cyberattacks than they think and the IT-security awareness is therefore relatively low.

5 Conclusion

The increasing damages caused by IT-security incidents pose a challenge for many companies. Recent studies show that the majority of successfully carried out cyberattacks require employee interaction, highlighting the critical human factor in cybersecurity. To investigate this human factor we built a mobile, scalable IT-security lab that enables study participants to experience realistic cyberattacks in an immersive workplace environment. We designed the platform in such a way that we can reach the target group of SME employees to ensure that the conducted studies are representative. We developed several demonstrators which, from our point of view, contain the most relevant cyberattacks for companies that require user interaction. The study participants experience a typical work environment with a corresponding fully functional workstation and typical workplace applications such as e-mail communication. As part of a first test setup we have conducted interviews that have shown that the cyberattacks of the developed demonstrators were experienced as realistic and that the overall concept is capable of increasing the level of IT-security awareness. The results show that the participants often overestimate themselves with regard to IT-security and that there is a need for measures to increase the IT-security awareness.

We think that the realistic recreation of a workplace environment and study participants from the target group enable us to carry out representative studies, however we don't know if participants will behave as they would in real cyberattacks. In addition, studies are only representative if participants include employees of a heterogeneous quantity of different company sectors and sizes.

After developing and testing our mobile IT-security lab, we will carry out studies to investigate the user behavior in the event of cyberattacks in detail and to be able to develop appropriate solutions to increase awareness for the respective attacks and remedial measures.

References

[Be22] Berg, A.: Economic Security Study. Bitkom e.V./, 2022.

[BSN19] Bada, M.; Sasse, A. M.; Nurse, J. R.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672/, 2019.

[Bu21] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz: Informationssicherheit mit System, Mar. 2021, URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, visited on: 02/24/2022.

[EL22] ELITE: Erlebbare IT-Sicherheit durch mobile IT-Sec.PopUp-Labs, 2022, URL: https://elite-projekt.de/, visited on: 05/02/2023.

[Fi18] Finnerty, K.; Motha, H.; Shah, J.; White, Y.; Button, M.; Wang, V.: Cyber security breaches survey 2018: Statistical release./, 2018.

[Gh18] Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T.: Security threats to critical infrastructure: the human factor. The Journal of Supercomputing 74/, pp. 4986–5002, 2018.

[Gj17] Gjertsen, E. G. B.; Gjære, E. A.; Bartnes, M.; Flores, W. R.: Gamification of Information Security Awareness and Training. In: ICISSP. Pp. 59–70, 2017.

[Hi17] Hillebrand, A.; Niederprüm, A.; Schäfer, S.; Thiele, S.; Henseler-Unger, I.: Aktuelle Lage der IT-Sicherheit in KMU. Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (wik)./, 2017.

[IS22] ISO Central Secretary: Information security, cybersecurity and privacy protection — Information security management systems — Requirements, en, Standard ISO/IEC 27001:2022, Geneva, CH: International Organization for Standardization, 2022, URL: https://www.iso.org/standard/82875.html.

[Mc17] McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M.: Individual differences and information security awareness. Computers in Human Behavior 69/, pp. 151–156, 2017.

[PJA21] Pulido, M. A.; Johnson, C. W.; Alzahrani, A.: Security Awareness Level Evaluation of Healthcare Participants Through Educational Games. International Journal of Serious Games 8/3, pp. 25–41, 2021.

[Sc18] Scholl, M.: Play the Game! Analogue Gamification for Raising Information Security Awareness. Systemics, Cybernetics and Informatics 16/3, pp. 32–35, 2018.

[Sh10] Sheng, S.; Holbrook, M.; Kumaraguru, P.; Cranor, L. F.; Downs, J.: Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI conference on human factors in computing systems. Pp. 373–382, 2010.